UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/675,652	09/30/2003	Jeyhan Karaoguz	15046US01	5798

23446 7590 02/13/2008
MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER	
POLTORAK, PIOTR	
ART UNIT	PAPER NUMBER
2134	
MAIL DATE	DELIVERY MODE
02/13/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/675,652	**Applicant(s)** KARAOGUZ ET AL.	
	Examiner PETER POLTORAK	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 December 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 December 2007* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Applicant amendment and drawings received on 12/03/07 have been accepted.

Response to Arguments

2. Applicant's arguments have been carefully considered.

3. In light of applicant amendments the 35 U.S.C. 112 rejection is withdrawn.

4. Applicant's arguments with respect to claims 1-10 and 18-28.

5. As per claims 1, 11 and 18, applicant argues that "it appears that the Examiner equates the 'media peripheral' limitation from Applicant's claim 1 with the service module disclosed by Anderson…" and that claims 1-28 are being based on inherency."

In order to clarify the examiner's rejection, the examiner points out that it is a device providing a Service (disclosed and named as such in Fig. 8.1) such as a printer or a copy-machine disclosed in 3.5.1 by Anderson that meets the limitation of the peripheral device claimed in claims 1, 11 and 18. As properly noted by applicant, Anderson also uses a term "service" that is a module enabling communication with the Service peripheral as shown in Fig. 7.1 and 8.1, for example.

In regard to applicant's reading an "inherency" in the rejection, the examiner clarifies that no inherency was suggested in the rejection, but rather the fact of obviousness. Although newly amended claims, as well as applicant's arguments directed towards the newly amended claims, are addressed in this Office Action below, the examiner brings applicant attention that claim 11 is substantially broader than claims 1 and 18. As a result, at least some of the arguments presented by applicant and directed towards claim 1, 11 and 18 are not present in the claim language of claim 11. For example, neither previous nor currently amended claim 11 recite “security data associated with a location of previous operation of the service module” that applicant argues on pg. 22 and that Anderson discusses in 72.2-7.2.3 (for example, a previously acquired marshaled object that contains the URL to the service).

6. Claims 1-28 have been examined.

Claim Objections

7. Claims 1-17 are objected to because of the following informalities: the recited methods steps do not clearly define the metes and bounds of the claimed limitations. For example, it is not clear whether the entity that acquires security data associated with the media peripheral is the same entity searching for a previously acquired security data, and is the same entity that exchanges information associated with the media peripheral, for example. The claim language should be clear and stand on its own, i.e. articulate the claimed invention. The steps of methods presented in claim 1-17 are difficult to follow as pertaining to the entities involved and relationship between the entities (and their interaction).

Appropriate correction is required.

Claim Rejections - 35 USC § 112

8. Claims 5, 7, 15, 22 and 24 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains

subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Applicant should provide the support for "authenticating said acquired security data prior to said searching" and “validating said acquired at least one identifier based on said previously acquired security data” in the specification or delete the newly introduced limitations.

Claim Rejections - 35 USC § 102

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

9. Claims 11 and 13-15 are rejected under 35 U.S.C. 102(e) as being anticipated by Larsson (USPN 7028102).

As per claims 11 and 13, Larsson discloses a method for establishing secure access to a media peripheral (printer 380) via a node (cell phone 100) in a communication network (10, see Fig. 1, for example). Larsson discloses detecting when the media peripheral is communicatively coupled to the node (see Fig. 11, steps 928 and associated text, for example), acquiring, upon said detection, security data (Printer Specification) associated with the media peripheral (Fig. 11, step 932/4 and associated text); and utilizing said acquired security data (step 936) to facilitate secure communication between the media peripheral and the communication network (steps 938/40 and associated, for example). Furthermore, Steps 906-914 disclosed in Fig. 11, clearly illustrate security data associated with the node used in facilitating the secure communication.

10. As per claim 14, Larsson discloses transferring said security data to a media exchange server (ISP) coupled to the communication network (step 936).

11. As per claim 15, it is clearly shown that the acquired security data is accepted only from an authenticated node (see steps 908 and 912).

12. Claims 11, 13-14 and 16-17 are rejected under 35 U.S.C. 102(b) as being anticipated by Anderson (Fredrik Andersson and Magnus Karlsson, "Secure Jini Services in Ad Hoc Networks", 2000).

    Anderson discloses a home network (Fig. 8.1) comprising a node (Lookup Server) and a media peripheral (e.g. printers or copy-machines, 3.5.1 disclosed as Service in Fig. 8.1).

13. As per claim 11, Anderson discusses a client offering a service (pg. 37) registering an offered service at the Lookup Server (pg. 41) by uploading a part of the service (Marshalled Object) to the Lookup Server. (7.2.1), which reads on: "detecting when the media peripheral is communicatively coupled to the node".

    The security data associated with the media peripheral is acquired by the node (Lookup Server acquires Marshalled Object, which contains an instantiation of variables to use in the downloaded service-proxy, see pg. 14 and Fig. 8.1) and, as step 3 of Fig. 8.1 clearly illustrate, that the said acquired security data is utilized to facilitate secure communication between the media peripheral and the communication network. Similarly, at least step 2 in the same figure clearly illustrate that the use of security data associated with the node (without at least device identification information attempting to lookup and download service would not be able to contact the node and, as a result, the request for the service download would never reach the node).

14. As per claim, 13, since the security data is originated at the media peripheral before distribution (and authentication) of the data over network this reads on "reading the security data from the media peripheral".

15. As per claim 14, the client downloading/using the service and disclosed in Fig. 8.1 reads on a media exchange server.

16. As per claim 16, the media peripheral is accessed after it is registered/initialized.

17. As per claim 17 Anderson discloses the node distributing data, such as (e.g. description of the service, etc.) for said registered media peripheral (7.2.2-7.2.3).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

18. Claims 12 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anderson (Fredrik Andersson and Magnus Karlsson, "Secure Jini Services in Ad Hoc Networks", 2000).

    Anderson teaches the Lookup Server acquiring security data and suggests using a certificate in order to authenticate a service offered by the media peripheral (8.2.3) and teaches the authentication of the certificate is authenticated by the recipient of the certificate using a public key (5.8, 8.2.3-8.2.4).

19. Anderson does not explicitly disclose that the node acquired security data comprises a digital certificate and that the security data associated with the node to facilitate secure communication comprises a public key. However, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a digital certificate in the node acquired security data and include a public key in the security data associated with the node given the benefit of enabling the node to authenticate the service offered by the media peripheral.

20. Claims 1-4, 6-7, 9-10, 18-21, 23-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anderson (Fredrik Andersson and Magnus Karlsson, "Secure Jini

Services in Ad Hoc Networks", 2000) in view of Pfaffenberg (Bryan Pfaffenberg, "Dictionary of Computer Terms", ISBN: 0-02-862884-5, 1999) or alternatively over Huston (USPUB No. 2002/0007402).

As per claims 1-2, 4, 6, 18, 20-21, 23, 26-28, Anderson discloses a home network (Anderson, Fig. 8.1) comprising a media peripheral (e.g. Anderson, printers or copy-machines, 3.5.1 disclosed as Service in Fig. 8.1), a media exchange server (Lookup Server) and at least one processor that acquires security data (certificate) associated with the media peripheral (see Anderson, Fig. 8.1 step 5 and associated text) that is used with previously acquired security data (Anderson, a marshaled object that contains the URL to the service, 7.2.2-7.2.3 and Fig. 8.1 step 3) to facilitate secure communication between the media peripheral in the home and the communication network.

21. Anderson does not explicitly recite: searching for previously acquired security data. However, an ordinary artisan would readily recognize that the service offered by the media peripheral are reusable (i.e. the client uses a printer more than once) and that each time the client will want to use network resources (such as a printer) the client must have an associated at least location information (such as provided in the acquired security data) with the resources. Furthermore, Pfaffenberg discloses the concept of storing previously used data (cache, Pfaffenberg, pg. 79-80). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to store the previously acquired security data given the benefit of improve the system's performance. Since cached data would not be the only data that is

stored in the system, a request of previously acquired security data would inherently include searching.

22. The limitation: “if said previously acquired security data is not found: said at least one processor exchanges information associated with the media peripheral, while the media peripheral is located in the home” is implicit. The examiner points out that in addition to computers data being corrupted, computers have limited amount of memory resources, including cache memory. This, problem is addressed in the art by clearing the cache entries as illustrated Adams (abstract, USPN 5873100), for example. Once, the previously acquired security data is deleted from the cache, the search for the acquired security data would not result in the desired information and the node would have to once again exchange information associated with the media peripheral as disclosed by Anderson in steps 2 and 3 of Fig. 8.1.

23. Additionally, as per claim 3 and 20, Anderson discloses the client reads said security data from the media peripheral (Anderson, step 4, Fig. 8.1).

24. Additionally, as per claims 25, the examiner considers saving the previously acquired data in the cache as reading on registering the data and points out that the previously acquired data comprises at least one identifier associated with the home (Anderson, a marshaled object that contains the URL to the service, 7.2.2-7.2.3).

25. As per claims 10 and 27, Anderson, Pfaffenberg and Adams do not explicitly disclose use of a previously established password during the exchange information. Official Notice is taken that the use of a previously established password during the exchange information is old and well known in the art of computer network security

(e.g. desktop authentication requesting network access resources such as Windows NT domain authentication) and an ordinary artisan at the time of applicant's invention would have been motivated to incorporate the password given the benefit of authenticating the requestor.

26. Claims 5 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anderson (Fredrik Andersson and Magnus Karlsson, "Secure Jini Services in Ad Hoc Networks", 2000) in view of Stallings (William Stallings, "Network Security Essentials: Applications and Standards", ISBN: 0130160938, 2000).

    Anderson discloses acquiring the security data and searching for the acquired security data as discussed above.

27. Anderson does not disclose authentication the acquired security data.

    Stallings discloses authentication of the acquired security data (Stallings, MAC and/or Hash, pg. 49-52). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include authentication of the acquired security data as disclosed by Stalling given the benefit of ensuring data integrity.

28. Claims 1, 3, 6-7, 11-13, 18, 20 and 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Handelman (USPub 2004/0016002).

    As per claims 1, 6-7 ,18 and 23-24, Handelman discloses at least one processor (an system processing a client request, e.g. a system comprising headend that includes Hardware Configuration Provider Unit 70, Fig. 1 or 2) that acquires security data (a representation of financial transaction details and/or a payment identification code that may be processed to enable billing of the user, [0095]) associated with the media peripheral (STB 45); said at least one processor searches for a previously acquired security data associated with a location of previous operation of the media peripheral (the headend then processes the payment identification code to bill the user [0095] clearly discloses that the headend must have some previously acquired security data corresponding to the security data. As per location, the examiner points out that in addition to some kind of address present in the previously acquired security data, which must be present for the user to receive billing data, which reads "a previously acquired security data being "associated" with a location of previous operation of the media peripheral, some kind of location of the equipment must be present in the system in order for the Hardware Configuration Provider Unit to be able to receive data). Handelman discloses that if said previously acquired security data is found, said at least one processor utilizes said acquired security data associated with the media peripheral and said previously acquired security data to facilitate secure communication between the media peripheral in the home and the communication network, after successful processing of the data (a successful transaction, *which inherently would involve at least associating and comparing the acquired security data and the previously acquired security data*, results in data being communicated to the media peripheral, e.g. [0099]).

29. Handelman does not disclose exchanging information associated with the media peripheral if said previously acquired security data is not found.

However, Handelman discloses generating a message indicating a successful transaction ([109]) and an ordinary artisan would readily recognize the need for a message indicating an unsuccessful transaction (i.e. if said previously acquired security data is not found) ability for the client to address the unsuccessful transactions (e.g. in order to resolve outstanding payments, addressing the account changes and/or discrepancies, etc.).

The examiner points out that generating a message indicating an unsuccessful transaction (e.g. account information invalid) is well known in the art of computing and electronic transactions. Similarly, the mechanisms enabling clients communicating information to address the discrepancies (e.g. credit card information to pay the outstanding payments, update an account information, etc.) are old and well known in the art of computing and electronic transactions (e.g. USPN 6546555, Internet transactions, etc.). Thus, generating a message indicating an unsuccessful transaction and enabling the client to communicating information in order to address an error associated with the transaction (which reads on: if said previously acquired security data is not found, exchanging information associated with the media peripheral, while the media peripheral is located in the home) are obvious variations that are well known in the art. One would have been motivated to use them especially in light of the benefits of these technologies as evidenced by their commercial success. (See KSR ruling).

30. Additionally, as per claim 11, receiving data (e.g. enabling the communication between the headend and the STP) reads on detecting when the media peripheral is communicatively coupled to the node. Alternatively, receiving pockets comprising the security data, which enables to acquire (retrieve) the included security data, also

reads on detecting when the media peripheral is communicatively coupled to the node.

31. As per claims 3, 13 and 20, the data must be read in order to be processed.

32. As per claims 28, although Handelman does explicitly recite that the at least one processor is one of a computer processor, a media peripheral processor, a media exchange system processor or a media processing system it is clear that the processor used in the method disclosed by Handelman not only is utilized by a computer but also handles media exchange transactions, and the examiner points out that assigning a specific name would not affect the functionality of the invention.

33. As per claim 12, Handelman does not explicitly teach that security data and the acquired security data comprise a device identification (ID). However, Handelma's invention is concern with a particular node configuration. Thus, it would have been obvious to an ordinary artisan at the time of applicant's invention to include a device identification in the said security data given the benefit of specifying the type of the device that configuration data is requested and to include the device identification in the previous security data given the benefit of ensuring the correctness of the request.

34. As per claims 7 and 24, the examiner considers validating the data (comparing said security data with the acquired security data) to read on authentication of the data.

35. Although, as per claim 11 and 18, Handelman does not disclose transferring said security data to a media exchange server

36. Claims 5 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Handelman (USPUB 2004/0016002) in view of Stallings (William Stallings, "Network Security Essentials: Applications and Standards", ISBN: 0130160938, 2000). Handelman discloses acquiring the security data and searching for the acquired security data as discussed above.

37. Hadnelman does not disclose authentication the acquired security data. Stallings discloses authentication of the acquired security data (Stallings, MAC and/or Hash, pg. 49-52). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include authentication of the acquired security data as disclosed by Stalling given the benefit of ensuring data integrity.

Conclusion

Although claims 8 and 25 overcame the prior art, the claims are rejected by virtue of their dependence.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free)

/Peter Poltorak/
Examiner, Art Unit 2134

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2132